Optimización en la implantación de salvaguardas o contramedidas en la Gestión de Riesgos. Normativa y herramientas habituales en España.

Vicente Jara Vera
Carmen Sánchez Ávila
Biometría, Bioseñales y Seguridad (GB2S), CeDInt
Universidad Politécnica de Madrid (España)
Email: vjara@cedint.upm.es, csa@cedint.upm.es

Javier Guerra Casanova
Alberto de Santos Sierra
Biometría, Bioseñales y Seguridad (GB2S), CeDInt
Universidad Politécnica de Madrid (España)
Email: jguerra@cedint.upm.es, alberto@cedint.upm.es

***Abstract*—La Gestión y Análisis de Riesgos supone en su fase final la toma de decisiones para reducir el riesgo en base a la adecuada selección de salvaguardas o contramedidas. Las metodologías y herramientas existentes (dedicando mayor espacio al análisis de los estándares ISO/IEC, MAGERIT, y la herramienta PILAR del CCN) han de permitir valorar unas salvaguardas frente a otras en base a una serie de variables medibles. En este estudio analizamos los estándares y herramientas más utilizadas y hacemos un análisis de situaciones cada vez más complejas, queriendo mostrar la dificultad de optar por las mejores opciones conforme los esquemas pretenden modelar la realidad, siempre compleja. La adición de nuevas variables llevará a la conclusión de cómo la normativa y las técnicas hoy en uso no son capaces de lograr una adecuada y óptima solución a los problemas de la toma de decisiones en la Gestión de Riesgos en los entornos de la Seguridad dentro de las Tecnología de la Comunicación y de la Información. El uso de la Optimización Matemática de la Investigación Operativa permite solventarlos de manera correcta, óptima, y muchas veces ofreciendo opciones alejadas de las soluciones que podrían parecer las adecuadas según las herramientas actuales.**

I. Introducción: Normativa para la Gestión de Riesgos en el ámbito de la Seguridad Informática y de las Comunicaciones

Sin ser exhaustivos en la amplísima normativa internacional existente, y centrándonos en la más extendida, implantada y que es referente, en el ámbito que nos atañe de la Seguridad Informática, indicar que en España la normativa que recoge los procedimientos relativos al análisis de riesgos es amplia, desde la Ley Orgánica 15/1999 del 13-diciembre-1999 de *Protección de Datos de Carácter Personal* [13] y el Real Decreto 263/1996 del 16-febrero-1996, *Regulador de la utilización de las técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado* [24].

Dentro del Análisis y Gestión de Riesgos (*Analysis and Risk Management*), las opciones que existen en España pueden condensarse en la ISO/IEC y MAGERIT, si bien existe otra normativa, recomendaciones y criterios de utilidad. Sucintamente, mencionemos:

- ISO/IEC serie-27000, sobre Seguridad de la Información (*Information Security*), donde el estándar 27005 trata sobre la Gestión de Riesgos (*Risk Management*) [9].
- ISO/IEC serie-20000, sobre Gestión de Servicio IT (*IT Service Management*) [10].
- MAGERIT (Metodología de Análisis y Gestión de riesgos de los Sistemas de Información) [14] es la metodología elaborada y usada por el Consejo Superior de Administración Electrónica (CSAE), órgano del Ministerio de Administraciones Públicas (MAP), que es el organismo encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del Gobierno Español, para la especificación de activos y sus riesgos asociados, y la implantación y uso de medidas que reduzcan y minimicen el riesgo, específicamente enfocada a las Tecnologías de la Información y la Comunicación dentro de las Administraciones Públicas. MAGERIT, cuya actual versión es la 2, es una Metodología de muy alta cualificación, que ha sido reconocida por ENISA (*European Network and Information Security Agency*). Como complemento a ella, el Centro Criptológico Nacional (CCN) ha desarrollado la herramienta PILAR (Procedimiento Informático-Lógico para el Análisis de Riesgos) para el fácil y mejor desarrollo de la Metodología, cuya actual versión es la 5.1 [5].
- UNE 71504:2008 de AENOR, Metodología de Análisis y Gestión de Riesgos para los Sistemas de Información [1]. AENOR (Asociación Española de Normalización y Certificación), como institución reconocida en los ámbitos nacional, comunitario e internacional para el desarrollo de sus actividades propias, y diseñada por Orden del Ministerio de Industria y Energía de España en el 1986, según Real Decreto 2200/1995, en desarrollo de la Ley 21/1992, de Industria, sigue muy de cerca a MAGERIT.

Otra normativa internacional, así como herramientas de amplio uso es:

- Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información, 2002 [23].

- NIST SP 800-30 del NIST, *Risk Management Guide for Information Technology Systems* [19].
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [20] [21].
- COBIT (*Control OBjectives for Information and related Technology*), de la ISACA (*Information Systems Audit and Control Association*) [12].
- OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), del CERT (*Computer Emergency Response Team*) de la Universidad de Carnegie Mellon, que es metodología, técnica y herramienta [25].
- CRAMM (*CCCTA Risk Analysis and Management Method*), de la CCTA (*Central Computing and Telecommunications Agency*), de amplio uso en entornos militares, como la OTAN [4].
- EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité*), creada por la DCSSI (*Direction Centrale de la Sécurité des Systémes d'Information*), del Ministerio de Defensa de Francia [7].

Mencionemos también normativa del Reino Unido, la cual ha sido de utilidad para la generación de otras, entre ellas la de España:

- BS 25999, *Business Continuity Management* [3].
- ITIL (*Information Technology Infrastructure Library*), ISPL (*Information Services Procurement Library*), ASL (*Application Services Library*), DSDM (*Dynamic Systems Development Method*) y CMM/CMMI (*Capability Maturity Model/Capability Maturity Model Integration*) [22].

II. Metodologías: entre Meta-metodologías y Herramientas

Los estándares ISO/IEC serie-27000 y en concreto la norma ISO/IEC 27005 [11] mencionados, no especifican ni recomiendan un determinado método o forma procedimental para la consecución de los objetivos de la gestión. Ofrecen un método estructurado, sistemático y riguroso para el análisis de los riesgos y la determinación de las políticas más adecuadas a seguir para minimizarlo. De manera deliberada el estándar recomienda que sean los propios usuarios del mismo quienes elijan los métodos (en plural) que mejor les convenga, ya sean métodos de estimación cualitativos o cuantitativos. Por otro lado hace notar que los métodos son de estimación del riesgo, no de definición del mismo. Sería así una meta-metodología. Indicar que hay multitud de sistemas propietarios cerrados y también abiertos que siguen las directrices ISO/IEC en este aspecto.

En referencia a MAGERIT, tenemos que decir que es también una meta-metodología, pero pretende llegar más allá, ofreciendo una guía documentada y amplia, con técnicas, procedimientos, consejos, casos prácticos y herramientas, como la mencionada PILAR del CCN.

La serie NIST SP 800-30 (*Risk Management Guide for Information Technology Systems*) puede ser vista como un marco generalista, a modo de una guía, mientras que 800-53 (*Recommended Security Controls for Federal Information Systems and Organizations*) es más procedimental y orientado a los controles o salvaguardas. Por otro lado, BS 25999 y EBIOS son recomendaciones y especificaciones de buenas prácticas, no teniendo el enfoque de herramienta sino el de meta-metodología, y con la suite de ITIL hay todo un marco de especificaciones, estándares, procedimientos, y todo tipo de herramientas para cada caso en concreto. Y finalmente, decir que COBIT, OCTAVE y CRAMM son netamente herramientas.

Nuestro análisis se enfocará al modo como se seleccionan las salvaguardas, contramedidas o controles a la hora de minimizar el riesgo, por lo que nos centraremos en cómo las herramientas llegan a realizar dicha selección. Veremos su procedimiento y algoritmia y especialmente nos centraremos en el caso español, con la herramienta PILAR del Centro Criptológico Nacional, aunque el enfoque se extenderá a todos ellos. A partir de las limitaciones encontradas ofrecemos nuestra propuesta -no novedosa, aunque no aplicada en estos escenarios- para lograr la adecuada selección de salvaguardas para los diferentes casos, metodología que será extensible en selecciones de alternativas que cumplan similares especificaciones y requisitos.

III. Escenarios

Supongamos un escenario genérico. En él tendremos una serie de activos $A = \{A_1, A_2, ..., A_a\}$, un conjunto de amenazas $Z = \{Z_1, Z_2, ..., Z_z\}$, diversas dimensiones de estudio del escenario $D = \{D_1, D_2, ..., D_d\}$, una serie de salvaguardas para minimizar algún tipo de riesgo $S = \{S_1, S_2, ..., S_s\}$, y ligadas a cada salvaguarda un coste de aplicación de cada una de ellas $CS = \{CS_1, CS_2, ..., CS_s\}$, así como la reducción del riesgo al aplicar cada una de las salvaguardas o contramedidas $RS = \{RS_1, RS_2, ..., RS_s\}$.

Habrá que suponer siempre el caso del presupuesto P finito, $P < \infty$. Hay que aplicar las salvaguardas que reduzcan el riesgo al máximo sin sobrepasar el valor del presupuesto, es decir, el coste de las salvaguardas elegidas. O sea, tomar un $S' \subseteq S / \ |S'| = l \leq s$ y $\sum_{i=1}^{l} CS_i \leq P$.

No tendremos en cuenta el caso dinámico temporal con un conjunto de ejercicios $E = \{E_1, E_2, ..., E_e\}$, sino que nos limitaremos al caso *hic et nunc*, siendo suficiente el adaptar los conjuntos A, Z, D, S, CS, y RS en cada instante temporal.

A. Escenario Salvaguarda, Coste, Reducción del Riesgo.

1) Primer ejemplo: Supongamos que sólo tenemos los conjuntos A, S, CS y RS, con los siguientes datos, de los que nos será indiferente la aplicación concreta sobre cada activo del conjunto A:

S	CS	RS
S_1	34	2
S_2	11	5
S_3	9	8
S_4	25	8
S_5	30	12
S_6	29	15
S_7	38	20
S_8	28	21
S_9	17	22

La situación será $max \sum_{i=1}^{l} RS_i * \delta_i$, con la restricción de coste $\sum_{i=1}^{l} CS_i * \delta_i \leq P$, donde $\delta_i = 1$ cuando tomamos la salvaguarda S_i, y 0 en caso contrario.

Suponiendo que pretendamos rebajar el riesgo al máximo sin sobrepasar el coste de, supongamos 60 unidades monetarias, podríamos empezar eligiendo la salvaguarda que más riesgo reduzca sin sobrepasar el presupuesto, lo que significaría tomar S_9. Seguidamente tomaríamos S_8. Luego S_3. Si hubiéramos optado por resolver este problema como un típico caso de Optimización Lineal Entera Mixta, MIP (*Mixed Integer Programming*) veríamos que ese es el resultado mejor, con un coste de $54u \leq 60u$, y logrando una reducción máxima del riesgo de $22, 21, 8$, pasando desde el riesgo inicial R_0 al final de $R_f = ((1 - 0,22)(1 - 0,21)(1 - 0,8))R_0$.

2) Segundo ejemplo: Con iguales condiciones, sea la tabla:

S	CS	RS
S_1	6	2
S_2	22	3
S_3	27	7
S_4	26	8
S_5	35	10

Si desde la visión de los datos tabulados tomamos en primer lugar la salvaguarda que reduzca el riesgo al máximo tomaríamos S_5, con un coste que no supera el presupuesto de 60. Pero si a continuación buscamos la mejor no podrá ser más que S_2, de ahí que la reducción del riesgo sea de $R_f = ((1 - 0,10)(1 - 0,03))R_0 = 0,873R_0$, con un gasto de $57u \leq 60u$. Sin embargo, la mejor solución es elegir S_1, S_3, S_4 con un coste de 59u, y un riesgo final de $R_f = ((1 - 0,02)(1 - 0,07)(1 - 0,08))R_0 = 0,8384R_0$.

B. Introducción de Dimensiones.

Lo habitual es trabajar sobre varias dimensiones, y en el caso del ámbito de la Seguridad Informática, las comunes son C (Confidencialidad), I (Integridad), D (Disponibilidad), A (Autenticidad), T (Trazabilidad), etc. Supongamos que nos quedamos con las más típicas, las tres primeras, C,I,D, por simplificar el escenario de ejemplos. Y supongamos también que tenemos los diagramas Kiwiatt siguientes, que son los que ofrece la herramienta PILAR del CCN en las gráficas de sus informes, y que MAGERIT denomina "diagramas de radar". Los gráficos de Áreas, Sectores, Líneas, Barras, Pila o Pareto son en lo básico similares a éste de Kiwiatt.

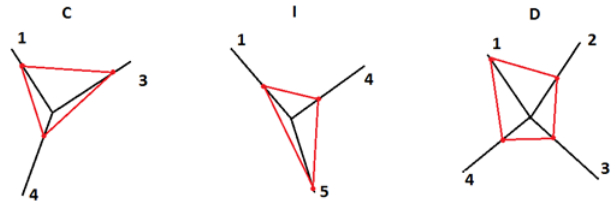

Fig. 1. Diagramas de radar de riesgo sobre las Dimensiones C, I, D

Supongamos la siguiente nueva tabla de datos:

A	D	S	CS	RS
1	C	S_1	6	2
4	I	S_2	22	3
2	D	S_3	27	7
3	C	S_4	26	8
5	I	S_5	35	10
4	C	S_6	61	13
1	I	—	—	—
1	D	S_7	65	15
3	D	—	—	—
4	D	—	—	—

La primera impresión, con el presupuesto disponible, si deseamos bajar el máximo riesgo sobre los activos es aplicar la salvaguarda S_5 sobre la dimensión I en el activo 5. El coste de 35 nos sitúa con un margen muy pequeño ante un total de 60 unidades monetarias, dejándonos sólo el usar la salvaguarda S_2 como mejor opción ahora.

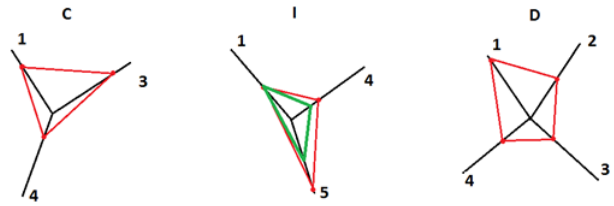

Fig. 2. Elección equivocada en la reducción del riesgo

Sin embargo, no es la mejor solución que bajaría en el total de dimensiones el riesgo. La elección óptima y correcta es S_1, S_3, S_4.

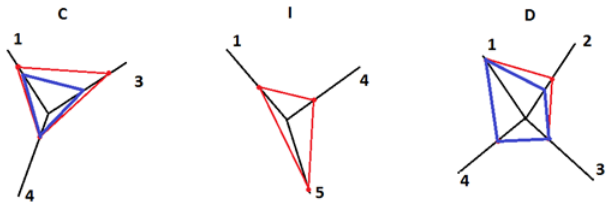

Fig. 3. Elección correcta en la reducción del riesgo

La toma de decisiones -sin sobrepasar los costes- basada en la sola representación gráfica de esquemas tipo Kiwiatt o similares puede llevar a optar por la reducción del riesgo en el aspecto donde aquél es máximo, y seguidamente y tras generarse el nuevo gráfico de Kiwiatt, volver a reducir en el que ahora será el nuevo máximo. Esta actuación secuencial no tiene por qué ser la mejor.

C. Introducción de reducciones de riesgo en función de las Dimensiones.

Sea la siguiente tabla, de un nuevo ejemplo:

S	CS	RS_C	RS_I	RS_D
S_1	34	7	26	0
S_2	11	0	0	18
S_3	9	0	33	3
S_4	25	17	0	23
S_5	30	3	29	9
S_6	29	11	24	0
S_7	38	0	29	0
S_8	28	13	4	15
S_9	17	22	0	0

Sobre el habitual presupuesto de $P = 60u$ intentemos reducir el riesgo, pero veamos previamente la reducción total aplicando $100(1 - [(1 - \frac{RS_C i}{100})(1 - \frac{RS_I i}{100})(1 - \frac{RS_D i}{100})])$:

Salvaguarda	Reducción total
S_1	31,18
S_2	18,00
S_3	35,01
S_4	36,09
S_5	37,32
S_6	32,36
S_7	29,00
S_8	29,00
S_9	22,00

Las salvaguardas a tomar son S_3, S_5, S_9, con coste de $56u$, y $R_f = ((1 - 0,3501)(1 - 0,3732)(1 - 0,22))R_0$.

D. Cuando el orden de aplicación de salvaguardas varía la Reducción del Riesgo.

Hasta ahora estábamos suponiendo que no importaba el orden de aplicación de las salvaguardas. No obstante, no es lo que tiene que ocurrir siempre con todas las salvaguardas y las reducciones de riesgos asociados. Habrá salvaguardas que si se aplican antes o después que otras supongan una reducción del riesgo en una o en varias dimensiones, en tanto que hay condicionamientos y solapamientos entre lo que algunas salvaguardas logran frente a otras. Deberíamos así construir las tablas de salvaguardas condicionadas por la aplicación previa de haberse tomado antes o durante otras salvaguardas. Veamos un ejemplo simple.

S	CS	RS
S_1	34	2
S_2	11	5
S_3	9	8
S_4	25	8
S_5	30	12

Supondremos que si se aplicara S_2 antes que S_5, ésta no reduciría ya, al aplicarse, el riesgo en su valor del 100%, pues ya ha sido aplicada S_2, las cuales salvaguardas suponemos que están relacionadas, sino que la reducción del riesgo que aportaría S_5 sería del 70% de su valor original. Similarmente, si se han aplicado ya las salvaguardas S_1 y S_4, supondremos que la apliación de la salvaguarda S_3 conseguirá paliar el riesgo en un 80% de su valor original. La situación será $max \sum_{i=1}^{l} RS_i * \delta_i$, con la restricción de coste $\sum_{i=1}^{l} CS_i * \delta_i \leq P$, donde $\delta_i = 1$ cuando tomamos la salvaguarda S_i, y 0 en caso contrario. Además, si $\{\delta_2 = 1 \wedge \delta_5 = 1\}$, $RS_5 = (1 - 0,3)RS_5$. Y si ocurre que $\{\delta_1 = 1 \wedge \delta_4 = 1 \wedge \delta_3 = 1\}$, $RS_3 = (1 - 0,2)RS_3$.

Nuestra situación ya no es del tipo MIP (*Mixed Integer Programming*), Programación Lineal Entera Mixta, sino del tipo MINLP (*Mixed Integer Nonlinear Programming*), Programación No-Lineal Entera Mixta.

Si no se tuvieran en cuenta estas consideraciones la solución óptima sería la aplicación de las salvaguardas S_2, S_3, S_5, con un coste de $50u$, y un riesgo final de $R_f = ((1 - 0,05)(1 - 0,08)(1 - 0,12))R_0$. Sin embargo, la situación correcta es aplicar S_1, S_2, S_3, con un coste de $54u$, ya que la aplicación del conjunto previo ofrecería realmente una $R_f = ((1-0,05)(1-0,08)(1-(\frac{0,12(100-30)}{100})))R_0$, no siendo la mejor opción, que pasa a ser la expuesta, S_1, S_2, S_3, con una $R_f = ((1 - 0,05)(1 - 0,08)(1 - 0,12))R_0$.

E. Tipos de riesgos: acumulados y repercutidos

Lo expuesto hasta ahora ha considerado el riesgo sin distinciones. Sin embargo, sabemos que el Riesgo acumulado se define como $R_A(a_i, t_j) = v(a_i)D(a_i, t_j)P_m(a_i, t_j)$, donde a_i es el activo i-ésimo; $v(a_i)$ es su valor acumulado (suma del valor propio y el valor heredado; t_j es la amenaza j-ésima; $D(a_i, t_j)$ es la degradación que provoca la amenaza t_j sobre a_i, y $P_m(a_i, t_j)$ su probabilidad de materialización.

Si aplicamos el mismo concepto sobre un activo en todas las amenazas posibles tenemos el Riesgo acumulado total sobre un activo i-ésimo que se expresa como $R_A(a_i) = \sum_{j=1}^{NA} v(a_i)D(a_i,t_j)P_m(a_i,t_j)$, donde NA es el número total de amenazas. Si ahora sumáramos este valor en todos los activos tendríamos el Riesgo acumulado total del sistema: $R_{Atotal} = \sum_{i=1}^{N}\sum_{j=1}^{NA} v(a_i)D(a_i,t_j)P_m(a_i,t_j)$, donde N es el número de activos del sistema.

Similarmente para los Riesgos repercutidos, $R_R(a_i) = \sum_{h=1}^{N}\sum_{j=1}^{NA} vp(a_i)Dep(a_i,a_h)D(a_h,t_j)P_m(a_h,t_j)$, donde $vp(a_i)$ es el valor propio del activo i-ésimo y $Dep(a_i,a_h)$ es la dependencia del activo i-ésimo sobre el h-ésimo. El Riesgo repercutido total del sistema será $R_{Rtotal} = \sum_{i=1}^{N}\sum_{h=1}^{N}\sum_{j=1}^{NA} vp(a_i)Dep(a_i,a_h)D(a_h,t_j)P_m(a_h,t_j)$.

Concluyendo: estas serán las distintas variables a estudiar, no ya sólo el riesgo "en general", sino el Riesgo acumulado (sobre un par activo-amenaza, sobre un activo, o sobre todos los activos); y el Riesgo repercutido (sobre uno o sobre todos los activos del sistema). Unos y otros nos darán información distinta, ya que los Riesgos acumulados nos indican por dónde tenemos las amenazas, sobre qué activos en concreto y qué salvaguardas conviene tomar preferentemente, mientras que los Riesgos repercutidos nos indican sobre qué partes del sistema con valor propio elevado recaen los riesgos, dándonos idea de la rentabilidad de aplicar las salvaguardas o no.

IV. La toma de decisiones en las metodologías del Análisis de Riesgos

Centrándonos en los más habituales en nuestro entorno, indicar que MAGERIT, en su documento I sobre el Método, da una serie de "consejos prácticos" en el apartado "5.6. Para seleccionar salvaguardas", en el cual pide que se use de un "catálogo de amenazas" y de un "sistema experto" para ver "la solución adecuada para cada combinación de tipo de activo, amenaza a la que está expuesto, dimensión objeto de preocupación y nivel de riesgo". Y no olvidar nunca elegir "una solución proporcionada a los niveles de impacto y riesgo calculados", así como "ponderar si el coste de la salvaguarda no supera el riesgo potencial"(pág. 99) [14]. En el documento de Técnicas, III parte del sistema MAGERIT, ninguna de las técnicas mencionadas, ya sean las específicas (Tabulación, Análisis Algorítmico, Árboles de Ataque), como las generales (Análisis coste-beneficio, Diagramas de Flujo de Datos, Diagramas de Procesos, PERT, Sesiones de Trabajo, el Método DELPHI, o la variedad de Técnicas Gráficas -GANTT, Puntos y Líneas, Barras, Radar, Pareto, Tarta, etc.) o bien no tienen directo uso para ayudar en la selección de salvaguardas, o bien no son método adecuado para la toma de decisiones, incluso cuando algunas de ellas se proponen como útiles para ello: así, los Árboles de Ataque son calificados como "una técnica para modelar las diferentes formas de alcanzar un objetivo"(pág. 22) [14], o especialmente en las Gráficas, que considera un "soporte en la toma de decisiones"(pág. 50) [14], si bien creemos haber mostrado suficientemente como son muy proclives a llevar a decisiones incorrectas.

PILAR, en su apartado "5.3.1.3.2. T.2 Salvaguardas" (pág. 108-111) [16], ofrece una serie de matices a las mismas, como el aspecto al que se refiere, la estrategia a la que pertenece, su importancia, su fuente, recomendaciones, aplicabilidad, dominio, herencia, etc, permitiendo además el uso de operaciones lógicas del tipo $\wedge$, $\vee$ y $\oplus$. Todos ellos aspectos importantes, pero incapaces de resolver un problema de Optimización Matemática. Así, en el apartado "5.3.1.3.2.2.1. Valoración automática de salvaguardas" encontramos una serie de ejemplos o situaciones incluso (pág. 126-128) [16] donde nos quedamos en aspectos de independencia, fases temporales de implantación y dominios, claramente mejorables. La gestión del riesgo está enfocado al modo de ensayo y error (pág. 31) [16], eligiendo una salvaguarda y mirando si conseguimos lo deseado frente a otras posibles.

Anotemos también la ausencia del uso del coste de las medidas de control y salvaguarda en el proceso procedimental de la herramienta, si bien PILAR es consciente claramente del coste detallado de las mismas, ya sea en la adquisición, la implantación, la instalación y configuración, el entrenamiento del personal y el mismo mantenimiento, como indica el apartado "7.8.3. Coste de las salvaguardas" del documento de Ayuda de la herramienta [15].

Y esto mismo encontramos en RMAT (*Risk Management Additional Tools*), versión 5.1, del Ministerio de Administraciones Públicas del Gobierno de España [17], en su apartado "7. Condición", el cual permite un uso de salvaguardas según amenaza, dimensión, o por pertenencia a herencia, clase, rango [min,max] de riesgo, y todo ello bajo un uso de operaciones lógicas o conectivas de la lógica proposicional del tipo $\wedge$ y $\vee$ (pág. 54-55). En definitiva, un entorno amplio, pero insuficiente.

En referencia al resto de meta-metodologías, metodologías y herramientas, si bien no puede encontrarse un acercamiento detallado a la selección de salvaguardas y contramedidas basado en la Investigación Operativa en los estándares ISO/IEC 27005, BS 25999, o en NIST 800-53, tampoco existen en las herramientas mencionadas previamente en este estudio, de amplio uso en el ámbito de Riesgos. Así, CRAMM [27] carece de la capacidad valorativa de costes y dependencias al nivel aquí especificado, siéndole imposible detectar la valoración óptima [18], pues incluso su método de evaluación iterativa y de prioridades, basado en gran parte en el uso de consultoría experta e información de cliente, así como el agrupamiento de contramedidas o salvaguardas en bloques,

creemos que sólo conlleva a enmascarar las soluciones acertadas impidiendo encontrar las mejores. Similarmente, la ISACA con su herramienta COBIT no parece percibir la dificultad de la toma de decisiones óptimas en sus escenarios de riesgo, o al menos esa es nuestra percepción, pues toda la parte dedicada al uso de salvaguardas, mitigación y priorización de las mismas parece desarrollarse sobre una concepción del modelo que aquí criticamos [8]. OCTAVE tampoco es una excepción dentro de la reducción del riesgo [18], ofreciendo un perfil demasiado cualitativo si bien tiene un sentido menos cerrado permitiendo diversas formas de lograr los objetivos de mitigación del riesgo [2].

V. Conclusión

Nuestro objetivo ha sido poner de manifiesto la toma errónea de decisiones en la metodología de Análisis de Riesgos (y posiblemente en otros ámbitos de la Administración ligada a las Decisiones), que implícitamente cree en la toma individual de una única opción en base a veces a muy prolija información, aunque mal gestionada, y en caso de no poderse satisfacer ésta, en la toma de la segunda, como mejor opción. Este método "natural" de actuar, cortoplacista, es de escasa profundidad de análisis y sumamente limitado, como hemos ido exponiendo de manera escalonada para mejor visualizar los errores habituales.

La metodología matemática de la Optimización y la evaluación de decisiones de la Investigación de Operaciones, sobradamente desarrollada, no es sin embargo una rama aplicada de manera consolidada a este ámbito del Análisis de Riesgos y la elección de contramedidas o salvaguardas para la seguridad en los entornos de las tecnologías de la Información y de la Comunicación [28], aun cuando vengan desde hace tiempo notándose las fallas de los sistemas habituales [26] y ofreciéndose soluciones muy novedosas incluso [29] [30]. Nuestro objeto ha sido indicar la persistencia de esta carencia en las metodologías y estándares existentes y habitualmente empleados en estos sectores, haciendo especial hincapié en España, mostrando cómo las actuales soluciones dejan recaer en las herramientas gráficas una irreal sensación de dominio del entorno, así como la forma de resolver de manera óptima y adecuada la parte correspondiente a la elección de controles y salvaguardas en la reducción del riesgo en los entornos de la seguridad [6]. Instamos así a la mención expresa de las técnicas de Optimización Matemática en las metodologías y estándares, así como su inserción en todas las herramientas -y esto ya sería desarrollo futuro para las versiones sucesivas- del Análisis y Gestión de Riesgos.

Agradecimientos

Los autores agradecen las ayudas del Ministerio de Economía y Competitividad para la realización de dicho estudio dentro de los programas del Centro para el Desarrollo Tecnológico Industrial (CDTI), inserto en el Proyecto CENIT Segur@, Seguridad y Confianza en la Sociedad de la Información, 2007/2004, en su apartado de "Análisis de Riesgos y Simulación de Crisis".

References

[1] AENOR, "UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información", 2008, http://www.aenor.es.
[2] Ch. Alberts, A. J. Dorofee, "Managing Information Security Risks: The OCTAVE Approach", en *Addison-Wesley Professional*, Boston, 2003.
[3] British Standards Institution (BSI), "BS 25999 Business continuity", 2010.
[4] Central Computing and Telecommunications Agency (CCTA), "CRAMM (CCCTA Risk Analysis and Management Method)", http://www.cramm.com.
[5] Centro Criptológico Nacional (CCN), "EAR/PILAR v5.1", https://www.ccn-cert.cni.es.
[6] R. J. Chapman, "Simple Tools and Techniques for Enterprise Risk Management", en *John Wiley and Sons*, Chichester, 2011.
[7] Direction Centrale de la Sécurité des Systémes d'Information (DCSSI), "EBIOS, Expression des Besoins et Identification des Objectifs de Sécurité", 1995.
[8] ISACA, "The Risk IT Practitioner Guide", ISACA, 2009.
[9] ISO27000, http://www.iso27000.es/download/doc_iso27000_all.pdf.
[10] ISO20000, http://normas-iso.com/iso-20000.
[11] ISO/IEC 27005, Information technology - Security techniques - Information security risk management , 2008.
[12] IT Governance Institute, "COBIT 4.1", 2007.
[13] Ley Orgánica 15/1999, "Protección de Datos de Carácter Personal", 13-diciembre-1999, http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html.
[14] Ministerio de Administraciones Públicas del Gobierno de España, "MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, v2", 2006.
[15] Ministerio de Administraciones Públicas del Gobierno de España, "PILAR, Análisis y Gestión de Riesgos. Documento de Ayuda, v4.3", 2008.
[16] Ministerio de Administraciones Públicas del Gobierno de España, "PILAR, Análisis y Gestión de Riesgos. Manual de usuario, v4.4", 2010.
[17] Ministerio de Administraciones Públicas del Gobierno de España, "RMAT, Risk Management Additional Tools. Manual de usuario, v5.1".
[18] T. Neubauer, "A Comparison of Security Safeguard Selection Methods", en *Proceedings of the 11th International Conference on Enterprise Information Systems, ICEIS 2009*, Springer, 2009, pp. 320–323.
[19] NIST, National Institute of Standards and Technology, G. Stoneburner, A. Goguen, A. Feringa, "SP 800-30. Risk Management Guide for Information Technology Systems", 2002.
[20] NIST, National Institute of Standards and Technology, "SP 800-53 Revision 3. Recommended Security Controls for Federal Information Systems and Organizations", 2010.
[21] NIST, National Institute of Standards and Technology, "Certification and Accreditation of Federal Information Systems Volume II: Part I - NIST 800-53 Rev 3; Part II - NIST 800-122", 2009.
[22] Office of Government Commerce (OGC), "ITIL, Information Technology Infrastructure Library", http://www.itil-officialsite.com.
[23] Organisation for Economic Co-operation and Development (OECD), "Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: Hacia una Cultura de Seguridad", 2004.
[24] Real Decreto 263/1996, "Regulador de la utilización de las técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado", 16-febrero-1996, http://www.boe.es/boe/dias/1996/02/29/pdfs/A07942-07946.pdf.
[25] Software Engineering Institute, Carnegie Mellon, "OCTAVE", http://www.cert.org/octave.
[26] K. J. Soo, "How Much Is Enough? A Risk-Management Approach to Computer Security", en *CRISP*, 2000.
[27] UK Government, "CRAMM User Guide. Version 5", 2005.
[28] J. Kounds, D. Minoli, "Information Technology Risk Management in Enterprise Enviroments", en *John Wiley and Sons*, Hoboken, New Jersey, 2010.
[29] L. P. Rees, J. K. Deane, T. R. Rakes, W. H. Baker, "Decision support for Cybersecurity risk planning", en *Decision Support Systems*, vol. 51, no. 3, 2011, pp. 493–505.
[30] V. Viduto, C. Maple, W. Huang, D. López-Peréz, "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem", en *Decision Support Systems*, online, pendiente aprobación, 2012.